INFORMATION SECURITY MANAGEMENT: AN EMPIRICAL ANALYSIS OF ITS CONSTITUTION

By

Daniel John Oost

A thesis submitted for the Degree of Doctor of Philosophy

School of Management, Faculty of Business

University of Technology, Sydney

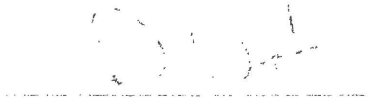
August, 2009

CERTIFICATE OF AUTHORSHIP/ORIGINALITY

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of candidate



ACKNOWLEDGMENTS

I would like to acknowledge the ongoing support and encouragement provided by my supervisor Professor Stewart Clegg and co-supervisor Professor Eng Chew. As the reader will shortly become aware, the support was provided not only in person but in book and journal form. I am greatly indebted to Professor Stewart Clegg's expert writings on the topic of power. Professor Eng Chew's wealth of experience as a practitioner provided an invaluable complement to this theoretical assistance.

Further, the coursework subjects led by Professor Carl Rhodes were an excellent preparation for my PhD work. I also valued the advice and support provided by Professor Carl Rhodes and Associate Professor Alison Pullen outside of the formal coursework setting.

I also need to express my gratitude for the generosity of the members of the participant organisation. The level of assistance provided and interest shown was a tremendous help.

Finally, I would like to thank my father, Jacob, and my Brother, Ben, for their proofreading efforts.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

Figures

Tables

ABSTRACT

This thesis addresses the following research questions:

> *How does analysis of the everyday discursive work of information security managers inform us about the phenomena that they constitute as 'information security?' What does it mean to 'do' information security?*

These questions are worth asking given the importance of information to organizations (Hong et al. 2003), the extent of current information security problems (Knapp et al. 2006a), a lack of empirical research on information security (Kotulic and Clark 2004), and a preponderance of research on technical solutions to information security problems conceived in technical terms (Dhillon and Backhouse 2001). In response to this situation some scholars propose simplistic 'cultural' solutions, without empirical basis.

To answer the research questions, and help address the abovementioned problems, I observed and recorded three months of weekly meetings of a group of information security managers at a large organization. The analysis of the data in order to develop answers to the research questions followed the reflexive interpretation approach advocated by Alvesson and Sköldberg (2000). The interpretive repertoire drawn upon to interpret the data and its relationship to my research questions centred on writings on power by Clegg (1989), Clegg et al. (2006a), Haugaard (1997), Hayward and Lukes (2008) and Lukes (2005), complemented by other resources.

The reflexively interpreted data, informed by the abovementioned writings on power, suggested that an integral part of the managers' 'doing' of information security involves the management of excess responsibility relative to their power to achieve a secure state. This is an inevitable dilemma given that a fundamental information security management problem, aside from the damage breaches cause for organizations, is that its very definition implies an unrealisable state. No system is completely secure (Straub and Welke 1998; Stewart 2004).

The management of responsibility took the form of devising authorised processes constituted by rules. The decision as to whether to act or not in relation to a potential information security problem is envisioned by the managers as a result of an application of rules, rather than individual agency. If an information security breach were to result (an ever present threat) the process would ideally be to blame, in effect absorbing the responsibility. However, rules require interpretation by agents (Clegg 1989) and are potentially subject to multiple interpretations. Agency and the management of its requisite responsibility cannot be escaped. A number of implications are developed as a result of this reflexive interpretation of the data, both theoretical and practical.